Department of Veterans Affairs

Memorandum

Date JUN 2 7 2006

From: Principal Deputy Under Secretary for Health (10A)
Chief Research and Development Officer (12)

Subj: Cyber Security and Privacy

To: VA Research Community

1. Secretary Nicholson has asked all VA offices and facilities to complete an inventory of all individuals (employees, contractors, volunteers) that have access to sensitive data on any of our data systems. Please note that VA's definition of sensitive information is quite broad (see: http://vaww.vhaco.va.gov/vadatarisk). You will be providing that information to your facility ISO over the next 2 weeks. ***We cannot overemphasize how important this survey is – we will be expected to provide accurate and complete information.***

2. The habits and practices for data security need to become second-nature for all of us - much like Universal Precautions for Prevention of Blood Borne Infections became for clinicians several years earlier. To assist in building these habits, VA has designated the week of June 26-30 as "VA Security Awareness Week." Each day of that week will feature locally-available educational activities and training materials designed to heighten our data security consciousness and reduce our risks. We ask each of the Research Offices to help publicize these local events to your local VA researchers, and to ensure that all understand the precautions that need to be taken in all cases, such as:

- ✓ Treating computers, removable or transportable electronic media, paper documents, and such, as if they contain sensitive data, and as if they could be stolen or compromised today,
- ✓ Using strong passwords,
- ✓ Storing as little sensitive information as possible on portable hardware,
- ✓ Encrypting the information I must carry around, and
- ✓ Physically securing all electronic media.
- ✓ These precautions apply regardless of the ownership or location of the computer or removable electronic media.

3. The other place to begin to learn about best practices is the mandated VA Cyber Security Awareness and VHA Privacy Policy training, which all VA employees must complete by June 30. ***Please note: this requirement includes all WOC and IPA research staff***. Additional guidance was provided through a recent memo dated June 12, 2006, from Dr. Kupersmith and Mr. William Feeley on research responsibilities for protecting sensitive information. The memo highlights the most recent policies for safe guarding our data.

4. There are also special rules regarding data security and privacy that pertain to research. These Handbooks and Directives are enumerated in the June 12, 2006 Memorandum. In implementing the policies and guidance you will be receiving in the coming weeks, all research offices and researchers will need to work closely with your local Information Technology Team, your Privacy Officer, and your Information Security Officer to ensure that all the data you use is protected from unauthorized disclosure or loss. Stay tuned for additional updates from ORD, which will be posted on our web site (www.research.va.gov).

5. We appreciate your commitment to ensuring information you have been entrusted with is safe and secure.

Michael J. Kussman
Michael J. Kussman, MD, MS, MACP

Joel Kupersmith
Joel Kupersmith, MD